MICROPROCESSOR SYSTEM AND METHOD FOR DETECTING THE EXCHANGE OF MODULES OF THE SYSTEM

Background Information

The present invention relates to the prevention of manipulations of microprocessor systems, in particular of engine-control devices for motor vehicles. Such devices are generally configured as microprocessor systems having a microprocessor, a

5   program and main memory for the microprocessor and one or a plurality of interfaces for the communication with sensors and actuators on the engine. By manipulating the control program of the processor, it is possible to influence the behavior of the engine so as to achieve higher engine output, for example. Power-output limitations, which are required to prevent possibly harmful overload

10   situations of the engine or which are mandated by law, may be circumvented in this manner. Consequently, there is a need for technology that makes unauthorized manipulations of such microprocessor systems impossible or at least makes them more complicated in a deterring manner.

15   One technique known and utilized for this purpose is the cementing of modules of such a microprocessor system. However, it has become apparent that no adhesive agent is available that is not able to be undone again in some manner. Another serious disadvantage of cementing is that it not only makes unauthorized manipulations more difficult, but repairs of the microprocessor system as well.

20

Summary Of The Invention

The present invention provides a microprocessor system and a method for exchanging a module in such a system, which make an unauthorized exchange much more difficult yet do not compromise the repair ease of the system. The

25   degree of difficulty is so high that in most cases the benefit obtainable by the manipulation does not justify the effort to be expended for this purpose, so that the manipulation makes no sense from an economical point of view.

The present invention is based on a microprocessor system having a plurality of

modules, among them a microprocessor and at least one storage module for storing the code and data for the microprocessor. At least one of the modules stores a serial number of this module in a non-changeable manner. It is common practice during the manufacture of microprocessors to provide them with a serial number that

5   is able to be queried with the aid of software, clearly identifies each microprocessor and cannot be changed in the finished microprocessor. Non-volatile memory modules, in particular flash memories, having serial numbers are available as well.

The present invention provides for a code number and information, in particular a

10   program code and a key, to be stored in the microprocessor, the code number having been obtained from the serial number of the at least one module identified by a serial number, with the aid of an encryption method. This information enables the microprocessor to calculate from the code number a serial number that should match the serial number of the module if the microprocessor system has not been

15   manipulated. In the event that the system was manipulated and the module has been replaced by another having, by necessity, a different serial number, this will be detected; appropriate measures may then be taken in that the microprocessor executes certain sections of its code provided for such an eventuality, for example, or refuses the execution of code sections that are relevant to its normal function. If

20   the microprocessor system is an engine control device and the vehicle has the appropriate equipment, including a display device, it is possible to display there a message for the driver that certain functions of the microprocessor system are blocked due to a fault in the system, or the system may prevent the start-up of the engine.

25

The encryption method by which the code number is obtained from the serial number is preferably an asymmetrical method, i.e., a method that uses different keys for encryption and decryption. The so-called public key used for decryption, which allows the serial number to be calculated from the code number in reverse,

30   may not be utilized for conversely calculating a code number from a serial number. Therefore, even if aware of the encryption and able to extract the public key stored in the system, an unauthorized person will be unable to determine from it a correct

code number that matches a serial number of a module he wishes to install in the system as replacement for a module that is marked by a serial number. As a result, no special measures are required to prevent an unauthorized person from extracting from the microprocessor system the information required for calculating the serial

5   number from the code number.

An important module of the microprocessor system which should be protected from unauthorized exchange is a storage module, in particular a storage module that includes the program code and/or parameter tables for the control task to be

10   implemented by the microprocessor system. The code number calculated from the serial number of such a storage module may be stored in just this storage module without endangering security.

Another module that is usefully protected according to the present invention is the

15   microprocessor of the system itself.

Storing the information required to calculate the serial number from the code number in the same storage module as the code number is inadvisable. An exchange of this module by an unauthorized person would be very difficult even when using the same

20   module for storage, due to the fact that, to be able to replace this module with an operative other module, this person would first have to understand the meaning of the individual data stored therein. Nevertheless, the separation provides an additional safety margin, since it is basically impossible for the exchange of a single module to remain undetected and the operativeness of the system to be maintained.

25   This makes it much more difficult for an unauthorized person to obtain information that would allow him to understand and circumvent the security measures through inspection of the microcomputer system.

In order to make it much harder for an unauthorized person to manipulate the

30   information required to calculate the serial number, the storage module containing this information is connected to the microprocessor system, preferably in an inseparable manner, possibly by integrating both in a one-chip microprocessor.

An additional security margin may be realized if, in those cases where the microprocessor system includes a plurality of modules, each of which is marked by a serial number, the code number is obtained by the joint encryption of these serial numbers. If this is done, a single decryption operation will suffice to ascertain in all

5   modules whose serial numbers have been entered into the code number whether or not they have been exchanged.

Brief Description Of The Drawings

Figure 1 shows a block diagram of a microprocessor system in which the present

10   invention is realized.

Figure 2 shows a block diagram of a second such microprocessor system.

Detailed Description

15   Figure 1 shows a block diagram of an engine-control device according to the present invention. Connected to a bus 1 on a printed circuit board are a microprocessor 2, a non-volatile storage module 3, a write-read memory module 4 and an interface 5 for the communication with sensors and actuators (not shown) of the engine to be controlled. Modules 2, 3, 4 are each formed by IC's which are separate from each

20   other. Non-volatile storage module 3 has a main memory location 6, addressable in a conventional manner, onto which the manufacturer of the engine-control device has written program instructions and parameter fields for microprocessor 2 and which is addressable in a conventional manner for reading via bus 1. Furthermore, storage module 3 includes a temporary memory location 7 onto which the

25   manufacturer of storage module 3 has already written a serial number that is specific to each individual storage module of a particular type. The content of temporary memory location 7 is readable via bus 1 as well, but the format of the address signals required to read out temporary memory location 7 differs from that for addressing main memory location 6. For example, to read temporary memory

30   location 7, it may be required, for instance, that a password be first applied to the storage module via bus 1. This excludes the possibility of replacing storage module 3 with a pin-compatible memory module delivered without serial number by the

manufacturer, in which only the serial number of storage module 3 has been copied into a conventionally addressable memory location. Module 3 may therefore be replaced only by a module of the same type, but different serial number.

5   Main memory location 6 of storage module 3 stores not only the program instructions and parameters required for the control tasks of the engine-control device, but also a code number and program instructions which microprocessor 2 is able to execute in order to calculate the serial number stored in temporary memory location 7 from the code number. This calculation is implemented at each start-up of

10   the system and/or in regular time intervals during its operation. If a comparison of the serial number calculated from the code number and the serial number in temporary memory location 7 shows that the two do not match, this indicates that storage module 3 must have been replaced. In this case, the program instructions stored in storage module 3 provide for a blocking of the operation of the control

15   device or at least a blocking of individual functions essential for the functioning of the engine it controls.

       If storage module 3 is a flash memory, such a blocking of functions is realized very easily in that the microprocessor applies a reset signal to storage module 3, which

20   deletes the data stored therein.

       An unauthorized person wishing to exchange storage module 3 for another in which the program instructions or parameters for microprocessor 2 are modified, may successfully accomplish this only by analyzing the program code contained in

25   module 3 and either modifying it in such a way that all checks of the serial number are prevented or by reconstructing the calculation of the serial number from the code number and entering a code number that matches the serial number in the storage module to be used as replacement.

30   A considerably greater security margin may be obtained if microprocessor 2 in the control device according to Figure 1 is replaced by a one-chip microcomputer 10 into whose one chip a microprocessor 12 and non-volatile program memory 11 are

integrated, which communicate via an internal bus that is not led out of the chip. If at all, access to the content of program memory 11 is possible only by opening the housing of the chip, which requires considerable effort and entails the danger of destruction of the chip. Program memory 11 includes a boot procedure for

5   microprocessor 12, which encompasses at least the calculation of the serial number from the code number stored in storage module 3, the reading of the serial number of storage module 3 and the complete or partial blocking of the control device if no match exists. Without access to microcomputer 10 itself, it is impossible to prevent the check of the code number in this case, so that a successful exchange of storage

10   module 3 requires the ability to determine the code number matching the serial number of the storage module to be installed. This is made virtually impossible for an unauthorized person if the manufacturer of the control device has used an asymmetrical encryption method to calculate the code number from the serial number of storage module 3. Such methods are known in great numbers, for

15   instance under the name of RSA (Rivest, Shamir, Adelman), Polig-Hellman, Diffie-Hellman, ElGamal, etc. All of these algorithms have in common that they use a secret key for encryption of a message, in this case, the serial number of storage module 3, and a public key for decryption of the message, and that the public key allows no conclusions to be drawn concerning the secret key and thus may not be

20   used to encrypt a message. That means that, even if the unauthorized person is able to read the key stored in program memory 11 and the program instructions for calculating the serial number from the code number using this key, this would still not enable him to construct the matching code number for a storage module 3 to be newly installed, which would convince microcomputer 10 to accept the exchanged

25   module as genuine.

The afore-described method for detecting the exchange of a module by calculating a serial number from a code number assigned to the module and by comparing the calculated serial number to the actual serial number of the module may easily be

30   generalized for a plurality of modules to be protected from exchange. For one, it is possible, of course, to store for each module an individual code number from which the serial number of the module may be calculated in reverse. It is more economical,

however, if the manufacturer encrypts a linking of the serial numbers of all modules that are to be protected and enters it into storage module 3 or some other suitable memory of the control device as a single code number that is valid for all modules. A one-time implementation of the decryption method will then suffice to calculate the

5   serial numbers of all protected modules. Since the calculation of the code number presupposes knowledge of all serial numbers of any modules that are to be installed and protected in the control device, and since it requires considerable effort to find out these serial numbers prior to assembly of the device, the control device is assembled first in this case; then, the serial numbers of all modules to be protected

10   are read out of the control device, the code number is calculated and only then is storage module 3 overwritten with the code number and all other data that is to be stored therein. If storage module 3 is an electrically overwritable memory, such as an EEPROM or a flash memory, it must be protected by a password in a manner known per se, so as to prevent manipulation of the data stored therein by an

15   unauthorized person, without storage module 3 being exchanged.